張貼日期：2022/10/18

【資安漏洞預警Fortinet FortiOSFortiProxy及FortiSwitchManager存在高風險安全漏洞(CVE-2022-40684)請儘速確認並進行更新或評估採取緩解措施

- 主旨說明Fortinet FortiOSFortiProxy及FortiSwitchManager存在高風險安全漏洞(CVE-2022-40684)允許遠端攻擊者繞過身分驗證程序取得管理者權限，請儘速確認並進行更新或評估採取緩解措施

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202210-0751
  - 研究人員發現Fortinet FortiOSFortiProxy及FortiSwitchManager之HTTP/HTTPS管理介面存在身分驗證繞過漏洞(CVE-2022-40684)此漏洞已遭開採利用，遠端攻擊者可藉由發送特製之HTTP(S)請求來觸發此漏洞，進而取得管理者權限。
- 影響平台：
  受影響版本如下：
  - FortiOS 7.0.0至7.0.6與7.2.0至7.2.1版本
  - FortiProxy 7.0.0至7.0.6與7.2.0版本
  - FortiSwitchManager 7.0.0與7.2.0版本
- 建議措施：
  1. 目前Fortinet官方已針對此漏洞釋出更新程式，請各機關儘速進行版本確認與更新：
     1. FortiOS請升級至7.0.7與7.2.2(含)以上版本
     2. FortiProxy請升級至7.0.7與7.2.1(含)以上版本
     3. FortiSwitchManager請升級至7.2.1(含)以上版本
     4. 若為FG6000F與7000E/F系列平台，請將FortiOS升級至7.0.5 B8001(含)以上版本
  2. 如未能及時更新，請參考Fortinet官方網頁之Workaround一節，採取下列緩解措施：
     1. 關閉HTTP與HTTPS管理介面。
     2. 限制可存取管理介面之IP
- 參考資料：
  1. https://www.fortiguard.com/psirt/FG-IR-22-377
  2. https://docs.fortinet.com/document/fortigate/7.0.7/fortios-release-notes/289806/resolved-issues
  3. https://docs.fortinet.com/document/fortigate/7.2.2/fortios-release-notes/289806/resolved-issues
  4. https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy
  5. https://www.helpnetsecurity.com/2022/10/11/cve-2022-40684-exploited/
  6. https://www.ithome.com.tw/news/153533

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20221018_01

Last update: **2022/10/18 10:49**